

AO 93 (Rev. 11/13) Search and Seizure Warrant

FILED  
RICHARD W. NAGEI  
CLERK OF COURT

## UNITED STATES DISTRICT COURT

17 JAN 13 PM 3:56

for the  
Southern District of OhioU.S. DISTRICT COURT  
SOUTHERN DIST OHIO  
WEST DIV CINCINNATIIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)One (1) ELECTRONIC STORAGE DEVICE FURTHER  
DESCRIBED IN ATTACHMENT A

Case No.

1:17MJ -28

## SEARCH AND SEIZURE WARRANT

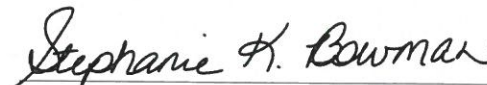
To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Southern District of Ohio  
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

**YOU ARE COMMANDED** to execute this warrant on or before January 27, 2017 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to Hon. Stephanie K. Bowman  
(United States Magistrate Judge)☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☒ for 30 days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_Date and time issued: 3:08 PM, Jan 13, 2017  
Judge's signatureCity and state: Cincinnati, OhioHon. Stephanie K. Bowman, U.S. Magistrate Judge  
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

AO 106 (Rev. 04/10) Application for a Search Warrant

FILED  
RICHARD W. HAGEL  
CLERK OF COURT

## UNITED STATES DISTRICT COURT

17 JAN 13 PM 3:56

for the  
Southern District of OhioU.S. DISTRICT COURT  
SOUTHERN DIST OHIO  
WEST DIV CINCINNATI

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)One (1) ELECTRONIC STORAGE DEVICE FURTHER  
DESCRIBED IN ATTACHMENT A

Case No. 1:17MJ -28

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 USC 2251, 2252

Illegal production, distribution, receipt and possession of child pornography

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jason Kearns, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.  
via electronic means.

Date: Jan 13, 2017

City and state: Cincinnati, Ohio

Judge's signature

Hon. Stephanie K. Bowman, U.S. Magistrate Judge

Printed name and title





IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF:  
One (1) ELECTRONIC STORAGE  
DEVICE FURTHER DESCRIBED IN  
ATTACHMENT A

Case No.

1:17MJ-28

**Affidavit In Support Of An Application Under Rule 41  
For A Warrant To Search And Seize**

I, Jason Kearns, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property— one (1) electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Homeland Security Investigations (HSI) Special Agent (SA), assigned to Cincinnati, Ohio. I have been employed with HSI as a Special Agent since September, 2005. As part of my duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have received training in the areas of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. In addition, I am a graduate of the Federal Law Enforcement Training Center (FLETC) Criminal Investigator Training Program (CITP), and Immigration and Customs Enforcement Special Agent Training (ICE-SAT), where I received training relative to conspiracy investigations, child pornography and



exploitation investigations, general smuggling investigations, smuggling of arms and strategic technology, confidential source handling, drug identification, federal drug law, and various surveillance and investigative techniques.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

**IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

4. The property to be searched is:

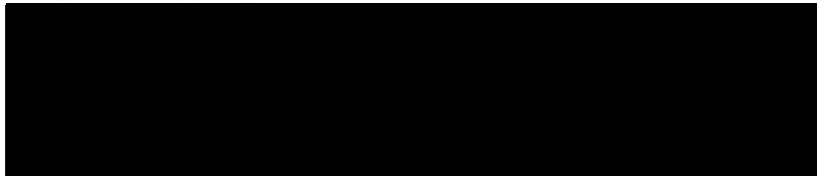
a. A Toshiba Satellite P745 laptop bearing serial number 2C382319K, herein referred to as "Device."

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

**PROBABLE CAUSE**

6. On December 23, 2014, the affiant received information from Detective Ken Volz of the Springfield Township Police Department (STPD). Detective Volz advised that they had a possible victim of child pornography in their area. Detective Volz further advised that the alleged suspect involved in coercing a minor to produce child pornography was [REDACTED] [REDACTED] was identified as a suspect in a previous HSI investigation. Detective Volz indicated that the incidents happened on or around December 19 and 20, 2014.

7. On December 24, 2014, the affiant conducted queries on [REDACTED] in several Law Enforcement Indices. The affiant verified that [REDACTED] was a previous suspect in an HSI investigation out of New Haven, Connecticut. A query of the Ohio Law Enforcement Gateway (OHLEG) for a valid Ohio driver's license was positive. OHLEG provided the following information on a valid Ohio driver's license:



8. On December 31, 2014, the affiant met with Detective Volz at the STPD. Detective Volz provided the affiant with a copy of the STPD report from the December 19th and 20th, 2014 incident. The following is a synopsis from the STPD report by Officer Martin Case on December 19th. The name of the victim was changed to Minor Victim 1 (MV1). The Hamilton County Communications Center received a text message from a sixteen year old boy stating that an adult male had explicit photos of the juvenile and was threatening to release them. Officer Case responded to the residence and was met at the door by the juvenile in question who identified himself as MV1. Officer Case explained to MV1's father that he needed to speak to his son regarding a crime that had occurred, but would fill him in as soon as he had a chance to speak to MV1 in confidence. MV1's father agreed. Officer Case then went to his patrol car and spoke with MV1 regarding the matter. MV1 explained that initially he was approached on a social media site called MeetMe. MV1 stated that the suspect was portraying himself as a young female under the handle [REDACTED]. The two began a conversation which led into MV1 sending nude photos of himself to [REDACTED]. Shortly thereafter the suspect made it known that he was not a young female, but in fact an adult male. The suspect then began stating that if MV1 did not agree to be his "boyfriend", he would post the explicit photos to all of MV1's twitter followers. MV1 then showed Officer Case the text messages between the two. The text messages were in short MV1 begging the suspect not to release the photos. MV1 stated that on December 19, 2014 he skyped with the suspect who appeared to be a black male or biracial male with a beard which appeared to be in his twenties. MV1 could only provide a Skype handle of [REDACTED] and the aforementioned MeetMe handle. MV1 also stated that he believed the

suspect's twitter handle was [REDACTED] MV1 was able to provide a mobile number from Skype of [REDACTED] Based on the information provided by MV1 and the phone number provided, Officer Case was able to locate a [REDACTED] in the Twinsburg, Ohio. Harrison also fit the description provided by MV1.

9. On December 20, 2014, STPD Officer Patrick Kemper responded to the station to see a complainant in the lobby. Officer Kemper met with MV1 who stated that they had previously reported an incident to Officer Case and additional messages had been sent to the victim. MV1 stated that he has been receiving text messages from the suspect all day and that after he failed to respond in a timely manner, the suspect stated he was going to post the pictures. After begging him not to post them, the suspect finally agreed not to. Officer Kemper spoke with Officer Case and Sargent Peterson about the incident and was asked to show a line up to MV1. After explaining the instructions to MV1, he began looking at the pictures. Upon opening folder number 4, MV1 stopped and gasped and stated that photo number 4 was the suspect. The individual in photo number 4 was [REDACTED] Officer Kemper asked him to look at the rest of the pictures before making a final decision. MV1 looked at the rest of the folders and then began looking through them once again, stopped at number 4, and stated he was 70% sure that was the suspect. When asked what about the pictures made him think that was the suspects, he stated that his hair and his facial hair were the same. Officer Kemper asked him what if anything made him unsure and he stated that he would recognize his voice. While Officer Kemper was searching the suspect through OHLEG, Harrison continued texting MV1 and continued to threaten to post the pictures online. MV1 became emotional and began crying in the lobby of the police department. After locating the suspect in OHLEG, Officer Kemper found an address in Twinsburg, Ohio. Officer Kemper contacted the Twinsburg Police Department and after briefing them on the investigation, asked them to attempt to locate [REDACTED]



██████████ Officer Kemper asked them to explain to ██████████ that an investigation was in progress and he was to have no further contact with the victim. If the photos were released, he would be facing additional felony charges. Officers from the Twinsburg Police Department responded to ██████████ and made contact with ██████████. Officers stated that ██████████ was acting very scared and stated that the message was clearly understood. Twinsburg officers obtained two contact numbers for ██████████ and one of those numbers ██████████ was the same number used for the skype session with the victim in paragraph 27.

10. On December 31, 2014 the affiant and Detective Volz met with MV1 and MV1's father. MV1 advised that on or about December 18, 2014, MV1 was utilizing the application MeetMe. He saw the profile for ██████████ which included three pictures of a female performing gymnastics. MV1 described ██████████ as a white female approximately 18 years old. ██████████ subsequently identified as ██████████ asked MV1 for his Kik username. MV1 and ██████████ started chatting on Kik. MV1 believed that ██████████ Kik username was ██████████ ██████████ asked MV1 to send him pictures of his calves and feet. MV1 indicated that he sent ██████████ a total of approximately 12 pictures of his calves and feet over the course of their chatting on December 18<sup>th</sup> and 19<sup>th</sup>. Sometime during their chat sessions, MV1 told ██████████ that he was still in high school. At one point, MV1 sent a picture of his entire body naked to what he thought was ██████████ ██████████ asked for his twitter name, which MV1 provided. ██████████ then told MV1 that he was a male and that if he did not become his "boyfriend" and send more pictures, then he would send the one picture of MV1 naked to every one of his friends on Twitter. During one of the conversations, ██████████ told MV1 that the ██████████ account was his friend's account that he was utilizing. Most of the chats consisted of MV1 begging ██████████ to not send the picture of himself naked to anyone. MV1 advised that

he was able to get the cell phone number for [REDACTED] from his Kik information. On December 19, 2014, MV1 had two conversations with [REDACTED] on Skype. The Skype chat provided the username of [REDACTED] and the name of [REDACTED]. As identified by OHLEG in paragraph 26, [REDACTED] middle name is [REDACTED] and his birthday is [REDACTED]. The first chat occurred at approximately 8:00 PM. [REDACTED] advised MV1 that he had already graduated high school, was a DJ, and raced a Subaru. MV1 also saw [REDACTED] face during this chat and the subsequent chat that MV1 believed took place sometime between 9:00 PM to 10:00 PM. During the second chat, [REDACTED] told MV1 that he would be safe and delete the picture if he did what he was told. [REDACTED] had MV1 get naked from the waist down and hump a pillow while he watched on Skype. He then had MV1 stand on his tip toes while again being naked from the waist down. After continuously receiving these threats, MV1 finally reported the incident to STPD. On December 20, 2014, MV1 had more conversations with [REDACTED] utilizing the Kik application. [REDACTED] continued to threaten MV1 that he would post the picture of him naked if he would not talk to him and be his boyfriend. MV1 went to the STPD to report it. This was when MV1 picked [REDACTED] out of a photo lineup.

11. On January 2, 2015, the affiant received information from HSI New Haven SA Ryan Mahar about a previous investigation against [REDACTED]. The West Hartford Police Department (WHPD) in Connecticut requested the assistance of HSI New Haven in July of 2013. The West Hartford Police Department advised that a 14 year old male, Minor Victim 2 (MV2) was blackmailed into sending nude photos over an internet messaging service, KIK. MV2 was contacted by Kik user [REDACTED] subsequently identified and herein referred to as [REDACTED]. [REDACTED] offered to send a nude picture of herself if MV2 sent a nude picture of himself first. MV2 agreed to the request, and sent a nude photograph of himself. MV2 stated that [REDACTED] then demanded additional nude photographs of MV2, and threatened to post the previous nude

photograph of MV2 to all MV2's friends on Instagram if MV2 did not comply. MV2 complied by sending additional nude photographs of himself, and [REDACTED] stated that MV2 should "go out" with her gay friend, [REDACTED]. [REDACTED] provided [REDACTED] telephone number as [REDACTED]. MV2 also advised WHPD that he exchanged text messages with [REDACTED] in which MV2 requested that [REDACTED] convince [REDACTED] not to post the nude photographs of MV2 on the internet. [REDACTED] advised MV2 that [REDACTED] would pay [REDACTED] not to post the nude photographs on the internet. MV2 told WHPD that MV2 received additional messages from someone identifying themselves as [REDACTED] but the messages came from different Kik accounts than the original account [REDACTED] used to correspond with MV2. During these conversations, [REDACTED] asked MV2 if he would like a nude photograph of her, and when MV2 replied affirmatively, [REDACTED] responded that MV2 was cheating on [REDACTED] and would post the nude photographs of MV2 on the internet. MV2 then received another request from [REDACTED] to send additional nude photographs of himself, and MV2 complied by sending additional nude photographs of himself. MV2 advised that [REDACTED] then demanded a nude video of MV2 humping a pillow in his long white socks, and if MV2 did not comply then [REDACTED] would post the nude photographs of MV2 on the internet. MV2 did not create this video and instead contacted [REDACTED] to request that [REDACTED] convince [REDACTED] not to post the nude photographs of MV2 on the internet. [REDACTED] told MV2 that [REDACTED] would pay [REDACTED] not to post the nude photographs of MV2 on the internet.

12. MV2 provided the following information about [REDACTED]. On Friday June 7<sup>th</sup>, 2013 MV2 made a Kik account and on Saturday June 8<sup>th</sup>, MV2 was contacted by [REDACTED]. She told MV2 that if he sent a full nude of his body, she would send one back. When MV2 did, she said keep sending them or I will post this pic on Instagram and follow all your friends so they can see. So MV2 said don't, I'll do anything. She then asked for pictures of MV2's legs. So MV2 sent them because he didn't want her/him to post it online. Then she said the last thing you



have to do is "go out" with my gay friend. So MV2 did. He knew his name as [REDACTED]. MV2 started texting to him and every time it got out of hand. MV2 could not persuade her to not post the naked pictures. [REDACTED] was saying that he was going pay her money not to post online. Then she made a new account and asked MV2 if he wanted pics and MV2 said yes. She said "that was a test you cheated on him so now Im posting it, bye". She made a new account with a different profile picture and a different name. Then she kept asking MV2 for pics of my legs. So MV2 sent pics of his legs. Also, twice she said that if MV2 does not send a video of himself naked, humping a pillow in long socks then she was going to post it. MV2 did not send her the video. MV2 went to the guy named [REDACTED] and he said that he would handle it and pay her again like he did the first time but he never did. It stopped there and MV2 did not hear from them. MV2 did not know if she posted the pictures on Instagram because he deleted Kik on Saturday June 8<sup>th</sup> at 12:00. She also said that she was from Cleveland, Ohio. [REDACTED] also gave me his number and his last name and middle name [REDACTED] and his phone number is [REDACTED].

13. On July 26, 2013, SA Mahar sent a Department of Homeland Security (DHS) Summons to Verizon requesting subscriber information and call history for telephone number [REDACTED] from 8/1/12 – 7/22/13. On August 10, 2013, Verizon Wireless provided information regarding telephone number [REDACTED] in response to a DHS Summons requesting subscriber information and call detail records. Verizon Wireless revealed that telephone number [REDACTED] is one of four telephone numbers listed in account number [REDACTED] which is subscribed to [REDACTED]. Information provided by Verizon Wireless also indicates that telephone number [REDACTED] is assigned to Device Identifier [REDACTED]. Searches in law enforcement databases conducted by SA Mahar revealed that a relative of [REDACTED] which

is the same first and middle name provided by the suspect, [REDACTED]

14. On August 29, 2013, Twinsburg Police Department (TPD) Detectives went to Twinsburg High School at 10084 Ravenna Road, in the City of Twinsburg to arrest [REDACTED]. This arrest was based on the information from the HSI New Haven investigation. [REDACTED] was located, arrested, and transported back to TPD. TPD Detectives took [REDACTED] to the interview room in the detective bureau where he was interviewed. [REDACTED] was read the Warning and Waiver of Rights form. [REDACTED] read the Waiver and then signed the form. [REDACTED] admitted that he currently had naked pictures of juvenile males on his phone. He also admitted that he has had a lot of naked pictures of juvenile males on his iPhone that he deleted. [REDACTED] admitted that he has sent and received a lot of naked pictures, too many to count or remember, using his iPhone. [REDACTED] uses the screen name of filthasorusrex when chatting on line. He has chatted with about 20-30 people at a time. [REDACTED] has made up fictitious names and profiles of people to have the victims send more naked photos to him. Two of those names being [REDACTED] and [REDACTED]. [REDACTED] mode of operation would be to contact an unknown party that he met on line, start a conversation with that person and after about 10 minutes, ask for a nude picture to be sent to him. If a picture was sent, he would tell the person that he was in a text conversation with, "Send me another one or I will send that one to your contact list." [REDACTED] would then introduce himself as someone else, through texting, and ask for pictures to be sent to him or help that person with not sending the naked picture to the other person. (Both of which were [REDACTED]). [REDACTED] admitted that he opened a KIK.COM account and has used that to communicate with different people from all over the United States. [REDACTED] stated that he is in a gay relationship with another male in Twinsburg. [REDACTED] would receive up to approximately 10 photos per day of naked full body shots of male juveniles. [REDACTED] stated that his iPhone number is [REDACTED]. [REDACTED] He is the only user on the phone and his mother or father pays the bill every month. [REDACTED]

has no idea how many people that he may have threatened with obtaining nude photos. He stated that he does not remember all of the names, user names, or where these individuals reside.

15. On January 12, 2015, the affiant met with MV1. MV1 advised the affiant that [REDACTED] had contacted him on January 10, 2015 on the MeetMe application. [REDACTED] was utilizing the username [REDACTED] MV1 advised that once he knew it was [REDACTED] he attempted to get screen shots of the conversation.

16. On February 18, 2015, the affiant conducted a query in google for the MeetMe usernames [REDACTED] and [REDACTED] The search indicated that the MeetMe username [REDACTED] had a userID of [REDACTED] The search for [REDACTED] did not return any results.

17. On February 24, 2015, the affiant served a DHS Summons on MeetMe for Registration Data, Account Notes, Connection Log, Profile Pictures for the following accounts:

[REDACTED]

18. On February 24, 2015, the affiant served a DHS Summons on Skype Communications for registration details: to include information captured at time of account registration and current e-mail address; Billing Address: User provided billing addresses; SkypeIn Current Subscription: List of SkypeIn numbers currently subscribed to by a User; Purchase History: Financial transactions conducted with Skype including billing addresses provided; Skype Out Records: Historical call detail records for calls placed to the public switched telephone network (PSTN); SkypeIn Records: Historical call detail records for calls placed from the public switched telephone network (PSTN); SMS Records: SMS text message historical detail records; Skype Wi-Fi Records: Historical Skype Wi-Fi records; E-mail & Password Records: Historical record of e-mail and password change activity for the Skype



username:

[REDACTED]

19. On February 24, 2015, the affiant served a DHS Summons on KIK for the last known customer names and email addresses and account creation dates for the account holders associated with the Kik usernames [REDACTED] IP addresses used by the account holders associated with the Kik usernames [REDACTED] and [REDACTED] Transaction histories for the account holders associated with the Kik usernames [REDACTED] and [REDACTED] Device type and manufacturer associated with the Kik usernames [REDACTED] and [REDACTED] "Elokowski" was the Kik username utilized by [REDACTED] to communicate MV1. The username [REDACTED] was obtained from the forensics conducted on MV1's cell phone.

20. On February 25, 2015, the affiant received a response to the aforementioned DHS Summons from Kik Interactive, Inc. Kik Interactive provided the following information:

First Name: deleted  
Last Name: deleted  
Email: [REDACTED]  
Username: [REDACTED]  
EST CLIENT\_VERSION 7.9.0.5000  
EST USER\_LOCATION US (city: Twinsburg, lat: 41.3152, long: -81.4405, tz: America/New\_York, ip: 76.188.82.184)  
EST REGISTRATION\_TIMESTAMP 2014/12/17 19:41:15  
EST USER\_LOCALE en  
EST REGISTRATION\_CLIENT\_INFO birthday=[REDACTED]  
EST REGISTRATION\_CLIENT\_INFO country-code=US  
EST REGISTRATION\_CLIENT\_INFO device-type=iphone  
EST REGISTRATION\_CLIENT\_INFO lang=en  
EST REGISTRATION\_CLIENT\_INFO model=iPhone  
EST REGISTRATION\_CLIENT\_INFO prefix=CIP  
EST REGISTRATION\_CLIENT\_INFO system-version=8.1.2  
EST REGISTRATION\_CLIENT\_INFO version=7.9.0.5000

21. On February 25, 2015, the affiant received a call from MeetMe, Inc. The representative of MeetMe advised that the profiles for the usernames laurenjapski and erinlakowski had been deleted by the user and no information would be available.

22. On February 26, 2015, the affiant conducted a query of the aforementioned Internet Protocol (IP) Address for [REDACTED] which was provided by Kik Interactive, 76.188.82.184. The query was conducted on whatismyipaddress.com. The following information was obtained:

IP: 76.188.82.184  
 Hostname: cpe-76-188-82-184.neo.res.rr.com  
 ISP: Time Warner Cable  
 Organization: Time Warner Cable  
 Services: None detected  
 Type: Broadband  
 Assignment: Dynamic IP.

23. On February 27, 2015, the affiant received a response to the DHS Summons, referenced herein, from MeetMe, Inc. MeetMe provided the following information for the MeetMe userID 112882359:

member\_id: 112882359  
 signed\_up\_at: 12/17/2014 20:56  
 registered\_at: 12/17/2014 8:56:09 PM  
 born\_on: 4/17/1996  
 registration\_ip\_address: 76.188.82.184  
 country\_code: US  
 removed\_at: 12/21/2014 5:39:13 AM  
 email\_address: [REDACTED]  
 removal\_reason: User Self-Delete

	logged_in_at	ip_address	device_type_name
	12/17/2014	76.188.82.18	
20:56	4		iphone
	12/17/2014	76.188.82.18	
20:58	4		iphone
	12/17/2014	76.188.82.18	
21:30	4		iphone
	12/18/2014	76.188.82.18	
5:24	4		iphone

	12/18/2014		70.208.200.5	
9:30		1		iphone
	12/18/2014		70.208.200.5	
10:57		1		iphone
	12/18/2014		70.208.200.5	
13:39		1		iphone
	12/18/2014		76.188.82.18	
16:09		4		iphone
	12/18/2014		76.188.82.18	
19:54		4		iphone
	12/18/2014		76.188.82.18	
20:01		4		iphone
	12/18/2014		76.188.82.18	
21:04		4		iphone
	12/19/2014		76.188.82.18	
1:27		4		iphone
	12/19/2014		76.188.82.18	
2:07		4		iphone
	12/19/2014		76.188.82.18	
2:56		4		iphone
	12/19/2014		76.188.82.18	
2:56		4		iphone
	12/19/2014		70.208.200.5	
13:01		1		iphone
	12/19/2014		76.188.82.18	
16:31		4		iphone
	12/19/2014		76.188.82.18	
17:12		4		iphone
	12/19/2014		76.188.82.18	
23:25		4		iphone
	12/20/2014		76.188.82.18	
0:03		4		iphone
	12/20/2014		76.188.82.18	
5:34		4		iphone
	12/20/2014		76.188.82.18	
6:10		4		iphone
	12/20/2014		76.188.82.18	
10:17		4		iphone
	12/20/2014		70.208.200.5	
11:08		1		iphone
	12/20/2014		70.194.230.5	
18:39		0		iphone
	12/21/2014		76.188.82.18	
4:59		4		iphone
	12/21/2014		76.188.82.18	iphone



5:37	4		
	12/21/2014	76.188.82.18	
5:38	4		Iphone

The registration IP Address was at approximately the same time and same date as KIK referenced herein.

24. On March 9, 2015, the affiant received a response to the aforementioned DHS Summons from Skype Communications referenced herein. Skype Communications provided the following account registration information for the Skype username: [REDACTED]

Username: [REDACTED]  
Acct Creation Time (in UTC): 2014-12-19 17:29:26.143 UTC  
Acct Creation IP: 70.208.200.51  
Acct Creation IP Country: United States  
Current Email Address: [REDACTED]  
Language At Reg: en

Skype Communications also provided the following password change information:

Username: [REDACTED]  
Change Date (in UTC): 2014-12-19 17:29:26.143 UTC  
Change Type: email  
New Value: [REDACTED]  
IP Address: 70.208.200.51.

25. On March 17, 2015, the affiant served a DHS Summons on Time Warner Cable for name, address, local and/or long distance telephone number, connection records or records of session times, duration, length of service (including start date) and types of services utilized; telephone or instrument number or other subscriber number or identity, including and temporary assigned network address; means of source of payment for such service (including any credit card and/or bank account number) for the following IP Address:

76.188.82.184 on 12/17/2014 8:56:09 PM EST

This was the registration IP Address and time from the information received from MeetMe referenced herein.

26. On March 18, 2015, the affiant received a response to the aforementioned DHS Summons from Time Warner Cable. Time Warner Cable provided the following account registration information for the aforementioned IP Address referenced herein.

Target Details 76.188.82.184  
Subscriber Name: [REDACTED]  
Subscriber Address: [REDACTED]  
Service Type - RR HSD Activate Date: 8/31/2013 Deactivate Date: Still Active  
User Name or Features: [REDACTED]  
Phone number: [REDACTED]

27. On May 27, 2015, a federal search was executed at the residence of [REDACTED]. The affiant and another HSI SA interviewed [REDACTED]. [REDACTED] read and signed a Statement of Rights form. [REDACTED] advised that he understood his rights and agreed to talk to the SAs. [REDACTED] advised that he was previously arrested by Twinsburg Police Department in 2014 for Extortion. He was sentenced to approximately one year of probation. [REDACTED] was 17 at the time. He was trading naked pictures, but he "thought it was cool because they were both underage". He admitted that he threatened individuals to get naked pictures. During this incident, he traded with an individual by the name of [REDACTED] but did not know his last name. Since December of 2014, [REDACTED] created fake profiles of 17/18 year old females on Meetme using his iPhone. He received a lot of responses from individuals above and below 18 years old. No less than 30 of the conversations and no more than 80 of the guys were below the age of 18. They would send [REDACTED] pictures of themselves of their full body naked. [REDACTED] would then request more pictures of the victim's flexing. If the victims did not send [REDACTED] more pictures of themselves naked, [REDACTED] would briefly upload the nude image to Twitter and then take a picture of the Twitter page. [REDACTED] would then tell the victim that if they did not send him more pictures of themselves naked, then he would share the Twitter page with the victim's friends.

██████ said that he did this approximately 20 to 30 times. Approximately one year ago, ██████, who was 18 at the time, was dating a 17 year old boy named ██████. ██████ received approximately 5 nude pictures from ██████ and sent him approximately two nude pictures. Around February of 2015, ██████ was dating an individual by the name of ██████. ██████ received approximately eight nude pictures from ██████ and sent him approximately two pictures of himself naked. ██████ admitted that he met approximately three more guys on MeetMe that were 16 to 17 years old. ██████ would Skype with them. During the Skype session, ██████ would have them flex and pose naked while he masturbated. ██████ then advised that when he was 15 years old, he started experimenting with his neighbor, who was an eight or nine year old boy. The neighbor's father caught them touching each other's privates. ██████ also admitted to utilizing the names ██████ and ██████ on Meetme. ██████ cell phone was seized and forensically analyzed. MV1's picture and phone number were located on ██████ phone. In addition, the item referenced in paragraph 4(a) was also seized and has been in law enforcement custody.

28. Based upon my knowledge, experience, and training in child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in these offenses:

- a. Those involved in the sexual exploitation of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in digital images, videos, or other visual media.
- b. Those involved in the sexual exploitation of children may collect



sexually explicit or suggestive materials, in a variety of electronic media. Individuals oftentimes use these materials for their own sexual arousal and gratification. Likewise, those involved in the sexual exploitation of children often maintain their cache in a digital or electronic format in a safe, secure and private environment, such as a computer or other electronic media.

- c. Those involved in the sexual exploitation of children often possess and retain their correspondence with their victims in the privacy and security of their home or some other secure location. These individuals typically retain this correspondence for many years.

29. There is probable cause to believe that the electronically stored information described in Attachment B may be recorded on the Device described in Attachment A. Your Affiant believes that the Device may contain evidence of the crimes referenced above.

30. The Devices are currently in the lawful possession of HSI. Therefore, HSI might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

31. I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of HSI.

#### **TECHNICAL TERMS**

32. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Hard Disk Drive(s) ("HDD"): are devices used for storing and retrieving

digital information. It is the customary device used for storage and secondary storage of data.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

33. In my training and experience, examining data stored on devices described in Attachment A, can uncover, among other things, evidence that reveals or suggests who possessed or used the devices and/or evidence of criminal acts and/or contraband.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

34. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on these devices. This information can sometimes be recovered with forensics tools.

35. There is probable cause to believe that things that were once stored on the electronic devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a

computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

36. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used,



the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

- a. data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information

on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to store evidence related to child exploitation, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

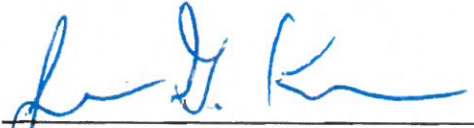
37. *Nature of Examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices as

referenced in Attachment A consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.


38. *Manner of Execution.* Because this warrant seeks only permission to examine the devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

**CONCLUSION**

39. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

  
\_\_\_\_\_  
Jason G. Kearns, Special Agent  
Homeland Security Investigations

Subscribed and sworn to before me this 13 day of January, 2017 via electronic means.

  
\_\_\_\_\_  
HON. STEPHANIE K. BOWMAN  
UNITED STATES MAGISTRATE JUDGE





**ATTACHMENT A**

The property to be searched:

1. A Toshiba Satellite P745 laptop bearing serial number 2C382319K

This warrant authorizes the forensic examination of the above property for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

All evidence on the Device described in Attachment A that relate to:

1. Violations of 18 U.S.C. §§ 2251(a), 2252 and 2252A.
2. Evidence related to sexual interest in minors, including but not limited to images and videos of minors engaged in sexually explicit conduct.